

-8-

## REMARKS

In response to the Office Action mailed on January 13, 2006 and further to the Advisory Action of May 12, 2006, Applicants respectfully request reconsideration in view of these remarks and amendments.

Claim 1-20 are currently pending in this Application.

Claims 2 and 15-19 are canceled.

Claims 1, 3, 4, 11 and 20 are herein amended.

Claims 21-26 are herein added.

Claims 1 and 11 and 26 are independent claims.

In the previous response, Applicants replied to the rejection of Claim 1 by suggesting that the interceptors in Kukura '923 are for receiving object invocations and passing control, while in contrast the claimed interceptors in the present application receive events (data) for selectively computing a decision to allow or block activity. The Office Action responds that such language is not recited in the claims. Applicants were characterizing the language in claim 1 which reads "plural interceptors identifying and governing the activity." Applicants submits that governing the activity and deciding whether to allow or block the activity describe the same operation, and deciding whether to "allow or block" the activity clarifies the recited "governing" of the activity. Nonetheless, Applicants have herein amended claim 1 to recite "selectively computing a decision to allow or block the activity," as suggested in the Office Action.

Further, the subject matter of claim 19 has been amended into claim 1, including intervening claim 2, to further refine applicants' claimed invention. The Office Action suggests that the claimed interceptors are disclosed in Kukura. Kukura '923, however, employs interceptors responsive to threading (control) rules, (column 15, line 16) not the claimed interceptors operable to receive a sequence of events indicative of requests for operating system resources. The claimed interceptors, therefore, receive events for computing a state. In contrast, the cited Kukura interceptors receive ORB invocations for accessing a predetermined service (col. 42:50-65). The interceptors in Kukura '923, therefore, are for receiving object invocations and passing control, while the claimed

interceptors in the present case receive events (data) for selectively computing a decision to allow or block activity, therefore governing the activity.

Further, the Kukura interceptors make no disclosure of state information, employed by the rule interpreter which applies the rule to the activity identified and the state information, also recited in amended claim 1. Accordingly, claim 1 is deemed allowable in view of the foregoing remarks and it is respectfully requested that the rejection under 35 U.S.C. §102 (e) be withdrawn in view of these remarks and amendments. Further Claim 11, rejected on similar grounds, has been likewise amended accordingly.

Claim 4 has been amended to recite that the stateful reference monitor computes a decision based on the processing policy defined by the rules to block or allow the event to be transmitted, as disclosed at page 10, lines 10-11. Claim 21 has been herein added to recite similar features with respect to Claim 11.

Claim 20 has been herein amended to recite that the plural reference monitors are operable to monitor at least two of file access, registry access, network access, object access, system call access, keyboard access, external inputs and user inputs, as disclosed at page 5, lines 15-18.

Claim 22 has been added to recite that the rules further comprise compiled rule byte code operable to perform selection of active rule set and an inactive rule set such that only a particular rule set is in effect at a particular time, as disclosed at page 12, lines 14-16

Claim 23 has been herein added to recited that the rule interpreting process is further operable to overwrite the rule byte code in a predetermined memory area and overwriting revised result byte code to effect a revised active rule set; the rule set operable for dynamic modification during persistent system operation, as disclosed at page 12, line 22-27 (i.e. without shutting down).

-10-

Claim 24 has been herein added to clarify that the rules defining allowable and disallowable activity further comprising a predetermined pattern of events and an identified prohibited pattern, as described at page 12, lines 28-31.

Claim 25 has been herein added to clarify that defining the identified prohibited pattern further comprises: operating in a state collection mode, the state collection mode operable for gathering normal patterns of activity, subsequently operating in a lockdown mode, the lockdown mode operable to detect and distinguish predetermined patterns of events and the gathered normal patterns of activity, and identifying detected patterns as unsafe based on user selection, as shown at page 12, line 30-page 13, line 7.

Claim 26 has been herein added to recite particular features of claims 1 and 21-25, to further clarify and distinguish the present invention.

As the remaining claims depend, either directly or indirectly from claims 1 or 11, which by the foregoing are deemed allowable, it is respectfully submitted that all claims now in the case are in condition for allowance.

Applicants hereby petition for any extension of time which is required to maintain the pendency of this case. If there is a fee occasioned by this response, including an extension fee, that is not covered by an enclosed check, please charge any deficiency to Deposit Account No. 50-3735.

-11-

If the enclosed papers or fees are considered incomplete, the Patent Office is respectfully requested to contact the undersigned collect at (508) 616-9660, in Westborough, Massachusetts.

Respectfully submitted,



---

Christopher J. Lutz, Esq.  
Attorney for Applicants  
Registration No.: 44,883  
Chapin Intellectual Property Law, LLC  
Westborough Office Park  
1700 West Park Drive  
Westborough, Massachusetts 01581  
Telephone: (508) 616-9660  
Facsimile: (508) 616-9661

Attorney Docket No.: CIS03-19

Dated: June 13, 2006